CVE Board Meeting – 20 March 2019

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.
Mark Cox, Red Hat, Inc.
Kent Landfield, McAfee
Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
Scott Moore, IBM
Lisa Olson, Microsoft
Kurt Seifried, Cloud Security Alliance
Ken Williams, Broadcom Inc.

Members of MITRE CVE Team in Attendance
Jo Bazar
Chris Coffin
Christine Deal
Jonathan Evans
Chris Levendis
Lew Loren
Cristina Padro
Joe Sain
Anthony Singleton

Agenda

2:00 – 2:15: Introductions, action items from the last meeting 2:15 – 2:30: Working Groups

- *Strategic Planning* – Kent Landfield/Chris Coffin
- *Automation* – Lew Loren
- *Cloud Security Alliance* – Kurt Seifried
- *Quality Working Group (QWG):* Dave Waltermire/Chris Coffin

2:30 – 2:45: Root CNA Update

- *MITRE* – Jonathan Evans
- *JPCERT* – Taki Uchiyama

2:45 – 3:00: Discontinuation of the cve@mitre.org **address (**Chris Levendis**)**

3:00 – 3:15: CVE Content Production System (CPS) Updates (Chris Levendis, Lew Loren**)**

3:15 – 3:30: Transitioning to JSON and XML download formats (Chris Levendis**)**

3:30 – 3:45: Discussion of Board communication (Chris Levendis**)**

3:45 – 3:55: Open Discussion – Board

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 6 February 2019

#	Action Item	Responsible Party	Status	Comments
1.23.1	Assemble additional operational guidance for program participation by CNAs (e.g., webinars, instructional videos).	MITRE (Evans/Sain)	In Process	MITRE assembled a list of guidance priorities and other areas of the program; the top five priorities are listed below: 1. How to submit entries to MITRE using the web form 2. CVE ID assignment rule (Counting) 3. Becoming a CNA 4. CVE Program (includes Root structure) How to request the MITRE CNA populate a CVE entry
1.23.2	Contact inactive CNA1 to determine the reasons for inactivity.		In Process	MITRE sent an email to CNA1 on February 6, 2019. Follow up email will be sent on February 20, 2019; if no response is received, CNA1 will be removed from the CNA program, consistent with the MITRE CNA Policies and Procedures (P&P) 1, "MITRE CNA Policy and Procedure for Inactive CNAs." **Update**: Response received from CNA1 on March 18th; still awaiting disclosure policy and advisory location. MITRE will respond to CNA1 again that a disclosure policy, advisory location, and submission of CVE IDs are requirements for participating in the CNA program. MITRE will request that CNA1 provide a disclosure policy and advisory location by April 8th, and if no response is received, CNA1 will be removed from the CNA Program on April 9, 2019.
1.23.3	Determine next steps for the DWF Root CNA.	MITRE/DWF/CVE Board	In Progress	Meeting was conducted on February 7, 2019. **Conclusions**: DWF is no longer sustainable and will stand down. MITRE will draft a community communication informing them of the change. MITRE will pick up DWF content production responsibilities while concurrently working with the Board to pursue alternatives. **Update**: Officially announced on March 7, 2019, via CVE Announcement, Twitter, and LinkedIn. Meeting with the DWF sub-CNAs the week of March 25 to ensure they understand CNA requirements.

#	Action Item	Responsible Party	Status	Comments
1.23.5	Work with Microsoft on starting the automated submission process.	MITRE (Evans/Sain/Coffin)	In Process	Microsoft to begin GitHub-based CVE submissions Tuesday, February 12, 2019. **Update**: The March data went through successfully March 20, 2019. The formatting of the data using the JSON format takes more iterations than expected (per Lisa Olson). Joe confirmed the test data was successful.
1.23.6	Send email to the Board list to initiate the CNA Rules revision process.	MITRE (Sain/Evans)	Completed	MITRE assembled a list of potential rules revisions and will perform internal review before sending to the Board. ▪ MITRE will draft proposed CNA Rules regarding EOL Scoping issue and Note Field in JSON. Target completion March 20, 2019. ▪ MITRE will draft proposed clarifications to CNA rules related to RBPs and send to the Board for review. Target completion February 28, 2019. **Update**: Jonathan Evans sent message to Board on March 21, 2019.
1.23.7	Contact GitHub to determine its interest in becoming a CNA.	Microsoft (Lisa Olson)	In Process	Lisa is working on this and updates the Board on progress. **Update**: Lisa is working with the MITRE team and will be following up with GitHub shortly.
2.6.1	Document new Inactive CNA Policy; post publicly and include in the new CNA rules and CNA onboarding process. Find a central location to store these types of policy changes.	MITRE (Levendis/Evans)	Completed	Document Final and sent to CVE Board on March 6, 2019.
2.6.6	Lew Loren from MITRE will contact Schmitty to explore the idea of splitting the work for CVE User Registry.	MITRE (Loren)	Completed	**Update**: Schmitty will continue to lead the conversations regarding the user registry and will elicit requirements from attendees; once the use cases and requirements are accepted, they will be handed over to the developers for implementation.
2.6.8	Coordinate a get together at RSA Conference with CVE Board members.	MITRE (Sain/Board)	Completed	MITRE invited all Board Members and the CNA to a get together on Monday, March 4th, 7:00 – 9:00 p.m.at the Grand Hyatt San Francisco.
2.6.9	Organize an event at Blackhat USA (August 2019) to celebrate 20 years of CVE.	MITRE (Evans/Sain/Bazar)	Assigned 2/6/19	Discuss with the CVE Board about event ideas for celebrating 20 years at CVE. **Update**: The Board agreed to assist in the preparation and planning of the event.

Working Group Updates

- Strategic Planning (SPWG) – Kent Landfield/Chris Coffin
  - The SPWG is continuing to review the Root CNA Roles and Responsibilities presentation. The group reviewed slides 13 through 18; review will continue at the next SPWG meeting on April 1, 2019, at 4:00pm EDT. The group agreed that the discussion about Root CNA roles and responsibilities has been valuable.
- Automation (AWG) – Lew Loren
  - ***CVE ID Allocation Services:*** Lew Loren explained that Schmitty will continue to lead the conversations regarding the user registry. Schmitty will be eliciting requirements from the attendees; once the use cases and requirements are accepted, they will be handed over to the developers for implementation.
  - ***AWG Meeting:*** The developers will be using this platform to showcase the progress being made in the Automation Services. Schmitty will provide a walkthrough of the outcomes from the Infrastructure and Architecture Definition Offsite Meeting held February 26 – 27.
  - Chandan Nandakumaraiah (Juniper Networks) requested changes to the JSON format originating from a pull request; this request will require overview and discussion from the community.
  - Kent noted that because of the planned migration to AWS, some of the services currently being developed may require temporary deviations from the designs (developed in the Offsite meeting) to ensure we build a bridge to the transition from old to the new version. Kent explained there are not enough resources to run them in parallel.
- Cloud Security Alliance Working Group (CSAWG) – Kurt Seifried
  - Final Survey will be sent shortly, and the next CSAWG meeting is scheduled for March 21, 2019 at 11:00am EST.
- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  - The second QWG meeting was held on March 13, 2019 at 2:00pm EST. This was the first meeting where there was community involvement, to talk about their use of CVE. Neal Slensker, VP of Vulnerability Analysis at Bank of America shared his use cases. Neal was given questions prior to the meeting to discuss his use of CVE and what his thoughts are on improving the program going forward. The input provided will help the QWG identify CVE use cases and prioritize efforts to improve the program.
    - Neal would like CVE information to be a real-time data feed of vulnerability information. He explained that it is important to have CVE details populated as soon as issues are public, and that vendors should publish their vulnerability information to the feed as soon as it is made public on their side.
    - Neal believes CVE IDs should only be provided when an issue is ready to publish, and they should not be used for coordination. He feels internal coordination can use bug tracking numbers, which would mean that the Reserved CVE status would no longer be needed.
    - The group agreed to collect feedback on how CVEs are used across the community.

- CNA Coordination Working Group (CCWG): Tod Beardsley/Chris Coffin
  - The CCWG in the process of nominating their Board liaison. The group agreed to invite the new CCWG Board liaison to the Board Meeting once the nomination is confirmed.

CNA Updates

- MITRE – Jonathan Evans
  - The Document Foundation was announced as a new CNA on March 15, 2019.
  - Introductory CNA Training sessions were held last week with OPPO and Bosch
  - Dell has submitted a request to spin Pivotal off as a separate CNA.
  - MITRE is working with DWF CNAs to transition to MITRE as their Root CNA. A meeting will be held, March 25, 2019.

- JPCERT - Takayuki Uchiyama
  - Jonathan spoke with Taki at the RSA Conference; Taki explained he is having issues bringing on new CNAs because of the requirement that CVEs must be submitted in English.

Special Topics

- Discontinuation of the cve@mitre.org address (Chris Levendis)
  - The cve@mitre.org email address was discontinued last week due to inactivity. MITRE sent contact information through the Board list that the Board can use to communicate with the CVE team.
- CVE Content Production System (CPS) Updates (Chris Levendis, Lew Loren)
  - The CPS was successfully deployed on Monday, March 18, 2019. The efficiencies have been immediately realized and the current CVE backlog will be worked off in the next few weeks.
- Transitioning to JSON and XML download formats (Chris Levendis)
  - Currently, there are 12 different download formats and accommodating so many formats is becoming unmanageable. The plan going forward is to move to two download formats, JSON and XML. MITRE will provide conversion tools to assist the community with this transition.
  - Kent L. noted that these transitions take a long time in the community because many tools may be impacted. The CVE ID format change took twelve months to complete due to the number of downstream users and tools that were impacted. Kent suggested a phased transition approach.
  - Mark C. suggested a download format that contains a *signer* field; currently this field is only available in Git. Mark believes that the formats should be definitive and complete. Art M. seconded this requirement.
  - The group agreed the timeframe for the data format transition would be a minimum of six months.
- CVE Website

- Chris explained the need to revamp the CVE website (https://cve.mitre.org/). The group discussed possible domain names for the next website. MITRE has already purchased several potential CVE domain names.

Open Discussion Items

- Rules Revision approach:
  - Jonathan E. will send the draft Rules Revision emails for the CVE Board to review and comment. Once feedback is received and incorporated, the rules revisions emails will be sent to the working groups for action.
  - The timeframe for when the working groups should have the rules revision completed will be determined by the CVE Board.
  - Chris L. recommended moving away from an annual review process and move toward an as-needed review process.

Action Items from Board Meeting held on 20 March 2019

#	Action Item	Responsible Party	Status	Comments
3.20.1	Document lessons learned from Microsoft automation submission process for other CNAs who want to move to GitHub automation process.	MITRE (Joe S.)	Not Started	Assigned 3/20/19
3.20.2	Send updated Root and Responsibilities Deck, with updates from SPWG March 18, 2019.	MITRE (Chris C.)	Not Started	Assigned 3/20/19
3.20.3	Work with Schmitty to reschedule AWG meeting using Skype instead of Microsoft Team Meeting.	MITRE (Lew L.)	Not Started	Assigned 3/20/19
3.20.4	Send notes from QWG held on March 13, 2019, and Briefer to the CVE Board email list.	MITRE (Chris C.)	Completed	Sent to CVE Board on March 20, 2019.
3.20.5	Send comprehensive list of the Working Groups and Leads to the CVE Board (Send to private CVE board if contact information is provided). Include the CNA Handshake Calendar that includes the meeting times and conference information for the Working Groups.	MITRE (Jo B.)	Not Started	Assigned 3/20/19
3.20.6	Record WG meetings moving forward so attendees that cannot attend can listen to the meeting recordings.	MITRE/WG Chair	Not Started	Assigned 3/20/19
3.20.7	Submit paper for Blackhat USA, call for papers due April 8, 2019.	Kent L/ Art M./MITRE	Not Started	Due April 8, 2019
3.20.8	Discuss how we can better handle the international community (English	CVE Board	Not Started	Assigned 3/20/19

	requirements of Guidance, Documentation, CVE IDs)			
3.20.9	Send a list of the domain names to the internal CVE Board list for review.	MITRE (Jo B.)	Not Started	Assigned 3/20/19
3.20.10	Check Handshake to confirm availability of historical recordings of Board meetings.	Kent L.	Not Started	Assigned 3/20/19
3.20.11	Review alternatives for public facing CVE Board discussion group archives.	MITRE (Joe S.)	Not Started	Assigned 3/20/19
3.20.12	Provide feedback/comment on the Rules Revision email (sent on March 21, 2019 at 1:51pm by Jonathan E).	CVE Board	Not Started	Assigned 3/20/19
3.20.13	Write up GDPR and GitHub issue.	MITRE (Lew L./Kent L.)	Not Started	Assigned 3/20/19

Board Decisions

- None

Future Discussion Topics

1) How can the program better communicate its future vision for the evolution and sustainability of the CVE program? How can CVE better market the CVE program and communicate the changes that are being implemented?
2) How can better status and metrics be provided to community stakeholders?
3) CNA Process – Front Door or Back Door: How should CNAs communicate with each other, and how would that information be managed?
   a) Set up an excel spreadsheet to share contact info amongst the CNAs
4) CNA Scope Issues
   a) The Board discussed that CNA documentation around roles and responsibilities are needed. Current documentation is not clear, CNAs assign and populate CVEs within their scope. Scope may or may not cover CVEs for their customers.
   b) CNA Rules - The rules state CNAs must be responsive but do not provide a specific time frame. The rules state if a CNA plans to assign a CVE for a vulnerability in another vendor's product, the assigning CNA should contact the vendor and give them the option to make the assignment. This must be clarified in the rule's revision process.
   c) Root CNAs - A given Root has a scope. A portion of the scope gets delegated to a CNA (i.e., product or area of research). If a portion of the scope is not delegated to a CNA, that scope stays with the Root. It is the Root's responsibility to assign and populate as the CNA of last resort.
   d) Action Item – CNA Rules must be updated to reflect this new approach.

5) Eliminate duplicate CVEs discussion
   a) The Board discussed that specifying CNA scope will help eliminate duplicate CVE assignments. Art explained that having open communication with other CNAs when making CVE assignments is critical; keeping this communication at the CNA level (not at Root/Primary level) will help prevent duplication.
      i) Recommendation 1: Process recommendation needs to be added to CNA guidance.
      ii) Recommendation 2: CNA rules must be updated to minimize duplicate assignments.
   b) Jonathan Evans explained that duplication of CVE assignments occurs the most with DWF.

6) Researcher CNAs
   a) The Board discussed researcher CNAs that have ambiguous scopes. These CNAs have issued thousands of CVEs.
      i) Recommendation 1: Avoid adding any new researcher CNAs until there are specific guidelines for what qualifies as a researcher CNA. This includes defined scope rules yet to be determined.
      ii) Recommendation 2: Make the scope naturally programmatic for researcher CNAs.
      iii) Recommendation 3: Change the process for researcher CNAs. Who is responsible for coordinating the assignment of the IDs? Who issues the CVE ID and who populates the information? There should be an easier way for companies to request a CVE ID.
      iv) Recommendation 4: Better define roles and responsibilities for researcher CNAs.
      v) Recommendation 5: Explore the possibility of researchers participating in the CNA program without becoming CNAs.
      vi) Recommendation 6: Need a testing/certification program for CNAs to make sure they can adequately perform their role, especially researchers.
   b) The Board agreed to explore better solutions regarding the researcher CNA ambiguous scope issue.

7) Operationalize Root CNAs effectively
   a) Further discussion is needed regarding how to operationalize Root CNAs more effectively.
   b) Additional discussion regarding MITRE's role in operationalizing roots is needed.

8) Product Type Tagging/Categorization
   a) As the production numbers for CVEs go up, there will be an increasing need to view a subset of the overall CVE master list
   b) Define a list of common product areas/domains to be used for categorizing CVE entries (e.g.., Medical devices, automotive, industrial, etc.)
   c) The tags/categories should be attached to the products and not to the CVE entries directly.
   d) Product listings in CVE User Registry would be a potential location.
   e) Can it be automated?

9) Future of CVSS
   a) Assigning multiple CVSS to a single CVE.
   b) Hill discussions around CVSS.